AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: _s/ Brandon Hale 05/31/2024

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Black 2GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon; Black 8GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon; Light blue/purple and white patterned universal storage bus (USB) electronic storage device, labeled SanDisk, and; Silver 4GB universal storage bus (USB) electronic storage device.

Case No. M-24- 484- AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, which is attached and incorporated by reference.

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Distribution and/or receipt of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of and/or access with intent to view child pornography (and attempt)
18 U.S.C. § 2251(a)	Sexual exploitation of children

The application is based on these facts:

See attached Affidavit of Special Agent Jesse Stoda.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jesse Stoda, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/31/24

Judge's signature

City and state: Oklahoma City, Oklahoma

Amanda Maxfield Green, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jesse M. Stoda, a Special Agent of the Federal Bureau of Investigation, Oklahoma City Division, being duly sworn, state:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since July 2017 and am currently assigned to the Lawton Resident Agency of the Oklahoma City Division. I first completed 22 weeks of training at the FBI Academy in Quantico, Virginia. During the training, I received instruction in a variety of investigative techniques commonly used in support of a wide range of the FBI's investigative priorities. The training included instruction regarding the use of confidential human sources, electronic and physical surveillance techniques, law enforcement tactics, search and seizure laws and techniques, interviewing strategies and skills, forensic techniques, and a variety of other subjects. While employed by the FBI, I have investigated various crimes, including, but not limited to, violent crimes against children. Based on my training and experience related to the investigation of child pornography and based upon interviews I have conducted with other officers, defendants, informants, and other witnesses and participants in child exploitation, I am familiar with the ways that child pornography is manufactured and distributed. My familiarity includes the various means and methods by which producers of child pornography manufacture and distribute pornography, their use of cellular telephones, computers, and other electronic devices. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal

laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

PURPOSE OF AFFIDAVIT

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) (distribution and/or receipt of child pornography (and attempt)); 18 U.S.C. § 2252A(a)(5)(B) (possession of and/or access with intent to view child pornography (and attempt)); and 18 U.S.C. § 2251(a) (sexual exploitation of children) are presently located within electronic storage devices (the "ELECTRONIC DEVICES"), that were located at 210 Cypress Avenue, Elk City, Oklahoma 73644, the residence of Amanda Kay Russell and Jonathon Chase Russell. I submit this Application and Affidavit in support of a search warrant authorizing a search of the ELECTRONIC DEVICES, as further described in Attachment A, incorporated herein by reference, and which are located in the Western District of Oklahoma. Located within the ELECTRONIC DEVICES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations further described in Attachment B, which is incorporated herein by reference.

3. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,

and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

g. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Records," "documents," and "materials," as used herein, include all

information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

IDENTIFICATION OF DEVICES TO BE EXAMINED

5. The property items to be searched are currently located at 410 SW 5th Street, Lawton, Oklahoma 73501, and are described as follows:

- Black 2GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon;
- Black 8GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon;
- Light blue/purple and white patterned universal storage bus (USB) electronic storage device, labeled SanDisk, and;
- Silver 4GB universal storage bus (USB) electronic storage device.

STATEMENT OF PROBABLE CAUSE

6. An FBI Online Covert Employee (OCE) operates in an undercover capacity on Swiss end-to-end encrypted application, TeleGuard. In that capacity, the OCE has established contacts with other international law enforcement officers (ILEO) who also operate in an undercover capacity on TeleGuard.

7. On January 30, 2024, the OCE was a member of a child pornography trading room on TeleGuard titled, "daughters nieces granddaughters real". On that date, the OCE observed TeleGuard user, toddylover, distribute 17 images that depicted the sexual abuse of two children. One of the images depicts an adult penis rubbing against the vagina of an approximately 3-year-old female. Another image depicts the lewd and lascivious display of the vagina of an approximately 11-year-old prepubescent female. Of the 17 images, 15 contained Child Sexual Abuse Material (CSAM) and two were non-CSAM images of the adolescent females.

8. On January 31, 2024, the OCE engaged in a direct messaging conversation with toddylover on TeleGuard. In the course of the direct messaging conversation, toddylover revealed that the two female children (those apparently sexually abused as depicted in the 17 images that toddylover distributed), were his nieces. Toddylover distributed three of the images, which toddylover had previously distributed to the OCE, in the direct messaging conversation. Toddylover went on to state that his nieces are three-years-old and 11-years-old, and that the two girls stay overnight with him between two and three nights per week. Toddylover further stated that on those nights, toddylover's

sister is working. In the messaging conversation, toddylover also stated, "about all I can do is cum on them when they're asleep. But they've definitely been absolutely covered in cum."

9. Over the course of January 31, 2024, to February 5, 2024, the OCE tried different methods to determine toddylover's true identity without success. As previously stated, TeleGuard is a Swiss end-to-end encrypted application, and these applications by nature do not maintain IP addresses or other subscriber information or content.

10. An ILEO provided the OCE with an Android push token as received from TeleGuard for toddylover. On February 5, 2024, subscriber information was requested for the Android push token from Google on an exigent basis. Google honored the exigent request and provided subscriber information for two different Google accounts that were associated with the push token, as well as related IP addresses.

11. The Google accounts were both associated with the cellular device bearing IMEI 866913061066541. Included in the Google subscriber information were three IP addresses, two of which resolved to Optimum (Suddenlink) and the other to Starlink. Subscriber information was requested from both Optimum and Starlink on an exigent basis. Both Optimum and Starlink honored the exigent requests. The information they provided showed that the IP addresses resolved to temporary lodging in Midland, Texas: one resolved to a TownePlace Suites, and the other resolved to Permian Lodging- Midland Lodge.

12. On February 6, 2024, an exigent request was served to AT&T for records associated with IMEI(s): 866913061066541, which identified cell phone number 432-

316-6767, subscriber Bob Lunger, and an address of 4300 E 50th St, Odessa, TX 79762; however, a cell phone location provided by AT&T showed that the phone was located at the Permian Lodging- Midland Lodge on February 6, 2024. Law enforcement database checks were unable to identify any person by the name of Bob Lunger, and the subscriber address, 4300 E 50th St, Odessa, TX 79762, resolved to a Microtel Inn and Suites. The use of the name Bob Lunger and the hotel address appeared to be an attempt to obfuscate the identity of the user of the Android device.

13. Based on the IP records obtained by Optimum and Starlink, FBI Agents requested the names of any hotel guests at the TownePlace Suites on the dates of June 11, 2023, and August 13, 2023, which were the dates that the Google accounts were created. Hotel staff provided a list of guests that were there on the corresponding dates. FBI Agents then requested Permian Lodging- Midland Lodge to check their guest list for any occupants from the provided names. JONATHON CHASE RUSSELL was identified as the only individual to have stayed at both the Permian Lodging- Midland Lodge and the TownePlace Suites on the noted dates and was located at Permian Lodging- Midland Lodge on February 6, 2024, in room SQ 27. Permian Lodging- Midland Lodge had RUSSELL's listed cell phone number as 940-257-9480 and that he was employed at Smart Oilfield Solutions. On February 8, 2024, Permian Lodging- Midland Lodge stated that RUSSELL had moved to a double occupancy room, EE 02, and would be checking out on February 10, 2024. An exigent request was served to Verizon Wireless for the cellular phone number provided, and in response, Verizon indicated a subscriber name of Jonathon Russell and a subscriber address of 210 Cypress Avenue, Elk City, OK 73644.

14. Law enforcement records fully identified the subject as JONATHON CHASE RUSSELL ("RUSSELL"), DOB: 08/XX/88. Exigent cell phone location records were provided from the dates of February 6, 2024, to February 8, 2024. During that time, FBI Agents observed that both cell phones 432-316-6767 and 940-257-9480 were collocated most of the time.

15. Through the investigation, agents learned that RUSSELL worked in Midland, Texas for certain weeks and, during his off weeks, he resided at his home in Elk City, Oklahoma.

16. Federal search warrant 24-MJ-031 was subsequently issued in the Western District of Texas authorizing the search of RUSSELL's premises in Midland, Texas. The search warrant was executed by federal agents on February 8, 2024. Several electronic devices were located and seized during the search. Child pornography was later identified on some of the devices. RUSSELL was also interviewed by agents that same night. During the interview, RUSSELL admitted to possession, distribution, and production of child pornography. Specifically, RUSSELL admitted to producing child pornography of one of his two minor daughters, Jane Doe 1 (JD1) so that he could trade it on the Internet.[1] RUSSELL was subsequently arrested by agents in the Western District of Texas pursuant to federal complaint 24-MJ-33.

17. On February 8, 2024, agents contacted and interviewed RUSSELL's wife, Amanda Russell, at their residence, 210 Cypress Avenue, Elk City, OK 73644. Amanda

[1] To agents' knowledge, he has not produced any child pornography of his nieces.

Russell provided consent for her residence to be searched by agents. Several electronic items were seized during the search. Additionally, several bedding sheets and furniture items bore the same appearance as child pornography previously distributed by RUSSELL. Those items were also seized by agents.

18. Amanda Russell also identified JD1 in some of the child pornography images found on RUSSELL's cell phone.

19. On February 9, 2024, RUSSELL's prepubescent biological daughters were forensically interviewed at the Child Advocacy Center (CAC) in El Reno, OK. Both of his daughters disclosed that RUSSELL had taken lewd and/or lascivious photos one of his daughters. Neither daughter disclosed that RUSSELL took pictures of JD1; instead, both daughters mentioned that RUSSELL took pictures of his other daughter, Jane Doe 2 (JD2). But agents have not located child pornography images of JD2.

20. On April 3, 2024, Indictment 24-CR-150 issued by a federal Grand Jury in the Western District of Oklahoma, charging RUSSELL with one count of sexual exploitation of a child in violation of 18 U.S.C. § 2251(a).

21. On May 28, 2024, I was informed by Amanda Russell that she had located additional electronic storage devices (the "ELECTRONIC DEVICES") in her residence at 210 Cypress Avenue, Elk City, OK 73644, that may have been utilized by RUSSELL. Amanda Russell consented for the FBI to search the ELECTRONIC DEVICES. She is not sure if the devices belong to RUSSELL or not.

22. The ELECTRONIC DEVICES are described above in paragraph 5 of this Affidavit. To the best of my knowledge and belief, none of the devices were manufactured

in the state of Oklahoma.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

25. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

26. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

27. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used

them, and when.

28. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

29. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO TRANSPORT, DISTRIBUTE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

32. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and

security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer or other electronic storage device in the surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[2]

---

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if the SUBJECT uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home.

CONCLUSION

33. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located on the ELECTRONIC DEVICES described in Attachment A. I respectfully request that this Court issue a search warrant for the ELECTRONIC DEVICES, authorizing the search and the seizure of the items described in Attachment B.

34. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated

in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Further Your Affiant sayeth not.

Jesse M. Stoda
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this the 31ST day of May, 2024.

Amanda Maxfield Green
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched includes the following devices, each of which was provided by Amanda Russell on May 29, 2024, and are currently located at the Lawton FBI Resident Agency, 410 SW 5th Street, Lawton, Oklahoma 73501.

- Black 2GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon;
- Black 8GB universal storage bus (USB) electronic storage device, labeled DataStick Pro by Centon;
- Light blue/purple and white patterned universal storage bus (USB) electronic storage device, labeled SanDisk, and;
- Silver 4GB universal storage bus (USB) electronic storage device.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

Contraband, evidence, fruits, and instrumentalities related to JONATHON CHASE RUSSELL distributing or receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2), possessing or accessing with intent to view material containing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), or sexually exploiting a child in violation of 18 U.S.C. § 2251(a), in any form, including, but not limited to:

1. Videos, still images, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

2. Written, typed, or verbal communications by or to RUSSELL that reflect how RUSSELL obtained, distributed, received, possessed, accessed with intent to view, or produced child pornography, or attempted to do the same;

3. Evidence of applications or other programs used to hide, obtain, access, or store images of child pornography;

4. Evidence of who used, owned, or controlled the device at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, user profiles, photographs, and correspondence;

5. Evidence of the times the device was used or accessed;

6. Passwords, encryption keys, and other access devices that may be necessary to access the the device and applications on the device;

10. Information or correspondence pertaining to affiliation with any child

exploitation websites or social media applications;

11. Any evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and

12. Evidence of the lack of such malicious software.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.